

1 Claims 53 and 70 are amended.

2 Claims 1-94 remain in the Application as follows:

3
4 **1. (Original)** A method comprising:

5 decrypting encrypted data that resides on one or more memory surfaces
6 associated with a video card, said act of decrypting being performed under the
7 influence of a cryptographic processor that resides on the video card, said act of
8 decrypting taking place only when an operation is to be performed on the data by a
9 graphics processor unit (GPU) that resides on the video card;

10 performing an operation on the decrypted data using the GPU to provide
11 resultant data;

12 re-encrypting, under the influence of the cryptographic processor, the
13 resultant data; and

14 writing the encrypted resultant data to a memory surface associated with the
15 video card;

16 at least one of said acts of decrypting and re-encrypting taking place on a
17 per cache page basis.

18 **2. (Original)** The method of claim 1, wherein the memory surfaces
19 reside on the video card.

20 **3. (Original)** The method of claim 1, wherein the acts of decrypting
21 and re-encrypting are performed using one or more block ciphers.

22 **4. (Original)** The method of claim 1, wherein the acts of decrypting
23 and re-encrypting are performed, at least in part, using one or more block ciphers
24 whose block size bears an integer size relation to a cache line of a cache page.
25

1 5. **(Original)** The method of claim 1, wherein the act of decrypting
2 and re-encrypting take place on a pixel-by-pixel basis.

3 6. **(Original)** The method of claim 1, wherein the cryptographic
4 processor comprises a hardware component mounted on the video card.

5 7. **(Original)** The method of claim 1, wherein the cryptographic
6 processor comprises an integrated circuit chip mounted on the video card.

7 8. **(Original)** The method of claim 1, wherein the cryptographic
8 processor comprises a trusted component.

9 9. **(Original)** The method of claim 1 further comprising receiving
10 pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one
11 or more memory surfaces.

12 10. **(Original)** The method of claim 1 further comprising receiving
13 pre-swizzled encrypted data that has been pre-swizzled by trusted software, and
14 writing the pre-swizzled encrypted data to the one or more memory surfaces.

15 11. **(Original)** The method of claim 1, wherein the act of decrypting
16 comprises caching decrypted pages in a local page pool cache to avoid multiple
17 decryptions if a same page is needed.

12. (Original) A method comprising:

decrypting encrypted data that resides on one or more memory surfaces associated with a video card, said act of decrypting being performed under the influence of a cryptographic processor that resides on the video card, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting, under the influence of the cryptographic processor, the resultant data; and

writing the encrypting resultant data to a memory surface associated with the video card;

said acts of decrypting and re-encrypting taking place on a per cache page basis.

13. (Original) The method of claim 12, wherein the memory surfaces reside on the video card.

14. (Original) The method of claim 12, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

15. (Original) The method of claim 12, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

1 16. **(Original)** The method of claim 12, wherein the act of decrypting
2 and re-encrypting take place on a pixel-by-pixel basis.

3 17. **(Original)** The method of claim 12, wherein the cryptographic
4 processor comprises a hardware component mounted on the video card.

5 18. **(Original)** The method of claim 12, wherein the cryptographic
6 processor comprises an integrated circuit chip mounted on the video card.

7 19. **(Original)** The method of claim 12, wherein the cryptographic
8 processor comprises a trusted component.

9 20. **(Original)** The method of claim 12 further comprising receiving
10 pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one
11 or more memory surfaces.

12 21. **(Original)** The method of claim 12 further comprising receiving
13 pre-swizzled encrypted data that has been pre-swizzled by trusted software, and
14 writing the pre-swizzled encrypted data to the one or more memory surfaces.

15 22. **(Original)** The method of claim 12, wherein the act of decrypting
16 comprises caching decrypted pages in a local page pool cache to avoid multiple
17 decryption if a same page is needed.

1 **23. (Original)** A method comprising:

2 decrypting encrypted data that resides on one or more memory surfaces of a
3 video card memory, said act of decrypting taking place only when an operation is
4 to be performed on the data by a graphics processor unit (GPU) that resides on the
5 video card;

6 performing an operation on the decrypted data using the GPU to provide
7 resultant data;

8 re-encrypting the resultant data; and

9 writing the encrypted resultant data to a video card memory surface
10 associated with the video card,

11 at least one of said acts of decrypting and re-encrypting taking place on a
12 per cache page basis.

13 **24. (Original)** The method of claim 23, wherein the acts of
14 decrypting and re-encrypting are performed using one or more block ciphers.

15 **25. (Original)** The method of claim 23, wherein the acts of
16 decrypting and re-encrypting are performed, at least in part, using one or more
17 block ciphers whose block size bears an integer size relation to a cache line of a
18 cache page.

19 **26. (Original)** The method of claim 23, wherein the acts of
20 decrypting and re-encrypting take place on a pixel-by-pixel basis.

21 **27. (Original)** The method of claim 23, wherein the acts of
22 decrypting are performed using at least one key that was received from a trusted
23 software component.

1 **28. (Original)** The method of claim 23 further comprising receiving
2 pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one
3 or more memory surfaces.

4 **29. (Original)** The method of claim 23 further comprising receiving
5 pre-swizzled encrypted data that has been pre-swizzled by trusted software, and
6 writing the pre-swizzled encrypted data to the one or more memory surfaces.

7 **30. (Original)** The method of claim 23, wherein the act of decrypting
8 comprises caching decrypted pages in a local page pool cache to avoid multiple
9 decryptions if a same page is needed.

10 **31. (Original)** A method comprising:
11 decrypting encrypted data that resides on one or more memory surfaces of a
12 video card memory, said act of decrypting taking place only when an operation is
13 to be performed on the data by a graphics processor unit (GPU) that resides on the
14 video card;

15 performing an operation on the decrypted data using the GPU to provide
16 resultant data;

17 re-encrypting the resultant data; and

18 writing the encrypted resultant data to a video card memory surface
19 associated with the video card,

20 said acts of decrypting and re-encrypting taking place on a per cache page
21 basis.

22 **32. (Original)** The method of claim 31, wherein the acts of
23 decrypting and re-encrypting are performed using one or more block ciphers.

1 **33. (Original)** The method of claim 31, wherein the acts of
2 decrypting and re-encrypting are performed, at least in part, using one or more
3 block ciphers whose block size bears an integer size relation to a cache line of a
4 cache page.

5 **34. (Original)** The method of claim 31, wherein the acts of
6 decrypting and re-encrypting take place on a pixel-by-pixel basis.

7 **35. (Original)** The method of claim 31, wherein the acts of
8 decrypting are performed using at least one key that was received from a trusted
9 software component.

10 **36. (Original)** The method of claim 31 further comprising receiving
11 pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one
12 or more memory surfaces.

13 **37. (Original)** The method of claim 31 further comprising receiving
14 pre-swizzled encrypted data that has been pre-swizzled by trusted software, and
15 writing the pre-swizzled encrypted data to the one or more memory surfaces.
16

17 **38. (Original)** The method of claim 31, wherein the act of decrypting
18 comprises caching decrypted pages in a local page pool cache to avoid multiple
19 decryptions if a same page is needed.
20
21
22
23
24
25

1 **39. (Original)** A system comprising:

2 means for decrypting, on a per cache page basis, encrypted data that resides
3 on one or more memory surfaces of a video card memory only when an operation
4 is to be performed on the data by a graphics processor unit (GPU) that resides on
5 the video card;

6 means for performing an operation on the decrypted data to provide
7 resultant data;

8 means for re-encrypting, on a per cache page basis, the resultant data; and

9 means for writing the encrypted resultant data to a video card memory
10 surface associated with the video card.

11 **40. (Original)** The system of claim 39, wherein the means for
12 decrypting comprises, at least in part, cryptographic hardware inside the GPU.

13 **41. (Original)** The system of claim 39, wherein the means for
14 performing comprises a GPU.

15 **42. (Original)** The system of claim 39, wherein the means for re-
16 encrypting comprises, at least in part, cryptographic processor hardware mounted
17 on the video card.

18 **43. (Original)** The system of claim 39, wherein said means for
19 decrypting and re-encrypting comprise one or more block ciphers whose block
20 size bears an integer size relation to a cache line of a cache page.

21 **44. (Original)** The system of claim 39 further comprising means for
22 pooling decrypted pages to avoid multiple decryptions of a page that might be
23 needed more than once.
24
25

1 **45. (Original)** A system comprising:

2 a video card;

3 a graphics processor unit (GPU) on the video card and configured to
4 process video data that is to be rendered on a display device;

5 memory on the video card comprising one or more input memory surfaces
6 configured to hold encrypted data that is to be operated upon by the GPU, and one
7 or more output memory surfaces configured to hold encrypted resultant data that is
8 to be rendered on the display device;

9 a cryptographic processor on the video card and configured to control
10 encryption and decryption on the video card, the cryptographic processor being
11 configured to enable encrypted data on one or more of the input memory surfaces
12 to be decrypted, on a per cache page basis, in connection with an operation that is
13 to be performed on the data by the GPU; and

14 the cryptographic processor further being configured to enable data that has
15 been operated upon by the GPU to be encrypted, on a per cache page basis, to an
16 output memory surface.

17 **46. (Original)** The system of claim 45, wherein the cryptographic
18 processor is configured to use block ciphers to effect encryption and decryption.

19 **47. (Original)** The system of claim 45, wherein the cryptographic
20 processor is configured to use one or more block ciphers whose block size bears
21 an integer size relation to a cache line of a cache page.

22 **48. (Original)** The system of claim 45, wherein the cryptographic
23 processor comprises a hardware component mounted on the video card.

24 **49. (Original)** The system of claim 45, wherein the cryptographic
25 processor comprises an integrated circuit chip.

1 **50. (Original)** The system of claim 45, wherein the cryptographic
2 processor comprises a trusted component.

3 **51. (Original)** The system of claim 45, wherein the cryptographic
4 processor is configured to set up a session key with a trusted software component.

5
6 **52. (Original)** A computer system embodying the system of claim 45.

7 **53. (Currently Amended)** A method comprising:
8 providing multiple input memory surfaces that are to hold encrypted data
9 that is to be processed by a graphics processor unit (GPU) on a video card;
10 associating, with each input memory surface, a decryptor that is uniquely
11 able to configured so as to decrypt the encrypted data that is held by the associated
12 input memory surface;

13 decrypting, with at least one associated decryptor, encrypted data that
14 resides on at least one respective input memory surface;

15 performing an operation on the decrypted data using the GPU to provide
16 resultant data;

17 re-encrypting the resultant data; and

18 writing the encrypted resultant data to an output memory surface associated
19 with the video card,

20 at least one of said acts of decrypting and re-encrypting taking place on a
21 per cache page basis.

22 **54. (Original)** The method of claim 53, wherein the act of providing
23 the multiple input memory surfaces comprises providing at least one input
24 memory surface on the video card.
25

1 55. (Original) The method of claim 53, wherein the act of re-
2 encrypting comprises using an encryptor that is uniquely associated with the
3 output memory surface to re-encrypt the resultant data.

4 56. (Original) The method of claim 53, wherein the act of re-
5 encrypting comprises using an encryptor that is uniquely associated with the
6 output memory surface to re-encrypt the resultant data, and wherein negotiated
7 key indices are used to identify and regulate which keys are used in decrypt and
8 re-encrypt operations.

9 57. (Original) The method of claim 53, wherein the acts of
10 decrypting and re-encrypting are performed using one or more block ciphers.

11 58. (Original) The method of claim 53, wherein the acts of
12 decrypting and re-encrypting are performed, at least in part, using one or more
13 block ciphers whose block size bears an integer size relation to a cache line of a
14 cache page.

15 59. (Original) The method of claim 53, wherein the acts of
16 decrypting and re-encrypting take place on a pixel-by-pixel basis.

17 60. (Original) The method of claim 53, wherein the acts of
18 decrypting and re-encrypting are performed under the influence of a cryptographic
19 processor that resides on the video card.

20 61. (Original) The method of claim 60, wherein the cryptographic
21 processor comprises an integrated circuit chip.
22
23
24
25

1 **62. (Original)** The method of claim 60, wherein the cryptographic
2 processor comprises a trusted component.

3 **63. (Original)** The method of claim 53, wherein the act of decrypting
4 is performed only when the GPU is to perform an operation on data that resides on
5 a particular input memory surface.

6 **64. (Original)** The method of claim 53 further comprising restricting
7 one or more operations that can be performed by the GPU based on whether
8 encrypted output is available.

9 **65. (Original)** The method of claim 53 further comprising decrypting
10 the encrypted resultant data for rendering on a display device.

11 **66. (Original)** The method of claim 53 further comprising decrypting,
12 with a display convertor, the encrypted resultant data for rendering on a display
13 device.

14 **67. (Original)** The method of claim 53 further comprising receiving
15 pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the
16 input memory surfaces.

17 **68. (Original)** The method of claim 53 further comprising receiving
18 pre-swizzled encrypted data that has been pre-swizzled by trusted software, and
19 writing the pre-swizzled encrypted data to the input memory surfaces.

20 **69. (Original)** The method of claim 53, wherein the act of decrypting
21 comprises caching decrypted pages in a local page pool cache to avoid multiple
22 decryptions if a same page is needed.
23
24
25

1 **70. (Currently Amended)** A method comprising:
2 providing multiple input memory surfaces that are to hold encrypted data
3 that is to be processed by a graphics processor unit (GPU) on a video card;
4 associating, with each input memory surface, a decryptor that is uniquely
5 ~~able to configured so as to~~ decrypt the encrypted data that is held by the associated
6 input memory surface;
7 decrypting, with at least one associated decryptor, encrypted data that
8 resides on at least one respective input memory surface;
9 performing an operation on the decrypted data using the GPU to provide
10 resultant data;
11 re-encrypting the resultant data; and
12 writing the encrypted resultant data to an output memory surface associated
13 with the video card,
14 said acts of decrypting and re-encrypting taking place on a per cache page
15 basis.

16 **71. (Original)** The method of claim 70, wherein the act of providing
17 the multiple input memory surfaces comprises providing at least one input
18 memory surface on the video card.

19 **72. (Original)** The method of claim 70, wherein the act of re-
20 encrypting comprises using an encryptor that is uniquely associated with the
21 output memory surface to re-encrypt the resultant data.

22 **73. (Original)** The method of claim 70, wherein the act of re-
23 encrypting comprises using an encryptor that is uniquely associated with the
24 output memory surface to re-encrypt the resultant data, and wherein negotiated
25 key indices are used to identify and regulate which keys are used in decrypt and
26 re-encrypt operations.

1 **74. (Original)** The method of claim 70, wherein the acts of
2 decrypting and re-encrypting are performed using one or more block ciphers.

3 **75. (Original)** The method of claim 70, wherein the acts of
4 decrypting and re-encrypting are performed, at least in part, using one or more
5 block ciphers whose block size bears an integer size relation to a cache line of a
6 cache page.

7 **76. (Original)** The method of claim 70, wherein the acts of
8 decrypting and re-encrypting take place on a pixel-by-pixel basis.

9
10 **77. (Original)** The method of claim 70, wherein the acts of
11 decrypting and re-encrypting are performed under the influence of a cryptographic
12 processor that resides on the video card.

13 **78. (Original)** The method of claim 77, wherein the cryptographic
14 processor comprises an integrated circuit chip.

15
16 **79. (Original)** The method of claim 77, wherein the cryptographic
17 processor comprises a trusted component.

18
19 **80. (Original)** The method of claim 70, wherein the act of decrypting
20 is performed only when the GPU is to perform an operation on data that resides on
21 a particular input memory surface.

22 **81. (Original)** The method of claim 70 further comprising restricting
23 one or more operations that can be performed by the GPU based on whether
24 encrypted output is available.
25

1 **82. (Original)** The method of claim 70 further comprising decrypting
2 the encrypted resultant data for rendering on a display device.

3 **83. (Original)** The method of claim 70 further comprising decrypting,
4 with a display convertor, the encrypted resultant data for rendering on a display
5 device.

6 **84. (Original)** The method of claim 70 further comprising receiving
7 pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the
8 input memory surfaces.

9
10 **85. (Original)** The method of claim 70 further comprising receiving
11 pre-swizzled encrypted data that has been pre-swizzled by trusted software, and
12 writing the pre-swizzled encrypted data to the input memory surfaces.

13 **86. (Original)** The method of claim 70, wherein the act of decrypting
14 comprises caching decrypted pages in a local page pool cache to avoid multiple
15 decryptions if a same page is needed.
16
17
18
19
20
21
22
23
24
25

1 **87. (Original)** A system comprising:

2 a video card;

3 a graphics processor unit (GPU) on the video card and configured to
4 process video data that is to be rendered on a display device;

5 memory on the video card comprising one or more input memory surfaces
6 configured to hold encrypted data that is to be operated upon by the GPU, and one
7 or more output memory surfaces configured to hold encrypted resultant data that is
8 to be rendered on the display device;

9 a cryptographic processor on the video card and configured to control
10 encryption and decryption on the video card, the cryptographic processor
11 comprising a key manager for managing keys that can be utilized for encrypting
12 and decrypting data on the video card;

13 each individual input memory surface having its own unique associated key
14 for decrypting encrypted data held thereon;

15 the cryptographic processor being configured to enable encrypted data on
16 one or more of the input memory surfaces to be decrypted on a per cache page
17 basis so that the decrypted data can be operated upon by the GPU;

18 the cryptographic processor further being configured to enable data that has
19 been operated upon by the GPU to be encrypted on a per cache page basis to an
20 output memory surface.

21 **88. (Original)** The system of claim 87, wherein the cryptographic
22 processor is configured to control encryption and decryption using block ciphers.

23 **89. (Original)** The system of claim 87, wherein encryption and
24 decryption takes place on a pixel-by-pixel basis.
25

1 **90. (Original)** The system of claim 87, wherein encrypted data held
2 on an input memory surface is decrypted only when it is to be operated upon by
3 the GPU.

4 **91. (Original)** The system of claim 87, wherein the cryptographic
5 processor comprises an integrated circuit chip.

6 **92. (Original)** The system of claim 87, wherein the cryptographic
7 processor comprises a trusted component.
8

9 **93. (Original)** The system of claim 87, wherein the cryptographic
10 processor is configured to set up a session key with a trusted software component.
11

12 **94. (Original)** A computer system embodying the system of claim 87.
13
14
15
16
17
18
19
20
21
22
23
24
25